Cassandra Crossing/ DTT e canali di ritorno

(19)—Altro che cookie sui siti governativi. Aumentano di continuo gli strumenti che mettono in mano a produttori e fornitori di servizi…

Cassandra Crossing/ DTT e canali di ritorno

(19)—Altro che cookie sui siti governativi. Aumentano di continuo gli strumenti che mettono in mano a produttori e fornitori di servizi molte più informazioni sull'utente di quanto questi ne sia consapevole.

20 gennaio 2006—Un recente caso di monitoraggio di chi naviga nella rete ed accede a siti del governo americano ha riacceso l'interesse sull'impiego dei cookie http per il tracciamento delle attività delle persone.

I cookie sono un argomento molto discusso, ma raramente dal punto di vista tecnico; per questo motivo la percezione dei rischi che la maggior parte delle persone ne ha, è molto imprecisa.

Semplificando, i cookie sono piccoli file (o record di un database, dipende dal browser che li gestisce) memorizzati nei personal computer in cui il server web a cui si ha accesso può leggere e scrivere informazioni, a futura memoria. Nascevano come mezzo per memorizzare informazioni allo scopo di migliorare l'user experience, permettendo ad esempio di non dover inserire password, di ritornare all'ultima pagina visitata o di offrire (vedi ad esempio Amazon.com) informazioni personalizzate agli utenti.

Ma i cookie sono anche utilizzabili (ed ampiamente utilizzati) per monitorare e profilare gli utenti; questo fatto è ormai noto, e per fortuna abbondano le

utility per gestirli e renderli “inoffensivi”. Anche un semplice uso attento delle funzionalità di base dei browser permette, utilizzandone le preferenze, di controllare e limitare l’uso dei cookie. I cookie, benché rappresentino un importante mezzo di raccolta di dati privati degli utenti, sono “oggetti” software, scritti (e cancellabili) sul disco del PC e neutralizzabili quindi con la massima semplicità.

Certo solo da coloro che voglio preoccuparsi della propria privacy…. ma questo è un altro discorso.

Fintanto che le minacce per la privacy sono realizzate tramite strumenti software, per l’utente esistono sempre possibilità di portarle allo scoperto e di trovare soluzioni alternative, come i software Open Source.

Quando pero’ il problema si trasferisce nel firmware (bios di schede ed apparecchi) od addirittura nell’hardware (Pentium D) queste possibilità si riducono moltissimo o scompaiono del tutto. Solo in rarissimi casi esiste firmware alternativo Open Source e libero, vedi il caso del bios Cromwell della console Xbox, e non esiste affatto “Hardware Libero”.

E comunque poiché un firmware libero dovrebbe girare su un hardware progettato da altri, la DMCA e leggi simili sono pronte ad impedirlo o renderlo difficilissimo. Si parla poi molto poco di altre e nuove possibilità di violazione della privacy degli utenti, che purtroppo aumentano continuamente di numero e di pericolosità; proviamo a giocare d’anticipo e descriverne una temibilissima, i canali di ritorno dei sintonizzatori televisivi.

Con la diffusione di massa delle nuove tecnologie di broadcast, come i ricevitori satellitari, ricevitori per il digitale terrestre e terminali cellulari per la videotelefonia DVB-H, il numero di oggetti di elettronica di consumo in grado di trasmettere dati su un canale di ritorno nascosto è letteralmente esploso, e presto essi entreranno in ogni casa ed in ogni tasca.

Consideriamolo come un effetto della transizione verso una società connessa.

Ma cosa è un canale di ritorno? Un canale di ritorno, ma forse sarebbe meglio definirlo appunto un canale nascosto, è la possibilità per un apparecchio ricevente, come ad esempio un ricevitore per il digitale terrestre, di trasmettere le informazioni che raccoglie interagendo con gli utenti.

Questo, con le tecnologie attuali, avviene solo per via telefonica utilizzando il modem incorporato nella maggior parte dei ricevitori satellitari e per il DTT.

Non appena un innocuo ricevitore (innocuo se escludiamo il tipo di contenuti che può fornire) viene collegato al telefono per consentire l’acquisto di film od eventi on demand, il canale di ritorno è aperto, e può trasmettere (e trasmetterà) i nostri dati a discrezione del gestore del sistema.

Ad esempio i ricevitori DTT che implementano le specifiche MHP permettono al gestore del sistema di caricare via radio un programma interattivo sul ricevitore, eseguirlo e ricevere i risultati di questo programma tramite il canale di ritorno (telefonico, ADSL, GSM….).

Sono gli stessi ricevitori venduti a milioni grazie anche ai finanziamento pubblici ed alla pubblicità martellante.

Una mega-AUDITEL che controlli ogni singolo click di qualsiasi utente, non solo del campione Auditel, è la prima cosa che vene in mente, il Grande Fratello è la seconda. Anche Orwell aveva immaginato un mondo in cui il tecnocontrollo si attuava tramite la televisione, ma nemmeno il Grande Fratello in persona avrebbe potuto sognare una cosa come i canali di ritorno degli apparati televisivi.

C'è speranza che le aziende che gestiscono e gestiranno tutto questo siano in grado di autoregolamentarsi?

Fatti accaduti anche di recente, ultimo il caso Sony/BMG, mostrano quanto le aziende abbiano a cuore gli interessi dei consumatori. Le aziende non sono in grado di autoregolamentarsi, non sono fatte per questo. Se avranno in mano un mezzo di questa potenza lo useranno al massimo delle loro possibilità.

Un intervento legislativo in questo senso è indispensabile, appropriato ed ancora tempestivo.

L'Autorità Garante della Privacy riterrà magari di intervenire in maniera propositiva verso il governo?

I politici, oggi in piena campagna elettorale, se ne prenderanno carico?

Originally published at punto-informatico.it.

Scrivere a Cassandra—Twitter—Mastodon
Videorubrica "Quattro chiacchiere con Cassandra"
Lo Slog (Static Blog) di Cassandra
L'archivio di Cassandra: scuola, formazione e pensiero

By Marco A. L. Calamari on August 26, 2023.

Canonical link

Exported from Medium on January 2, 2024.